

## Data Retention Policy

<b>Version Number</b>	2
<b>Revision Date</b>	September 2025
<b>Department</b>	Governance & Transformation
<b>Author</b>	Business Support Officer – Risk & Governance
<b>Reason for Policy Creation/Revision</b>	Planned review as part of the GDPR improvement project
<b>Data Protection</b>	This policy complies with UK Data Protection legislation
<b>Equalities Impact</b>	Not required at this stage
<b>Sustainability Impact</b>	
<b>Proof Read By</b>	Head of Governance & Transformation
<b>Date Approved</b>	30 October 2025
<b>Approved By</b>	SMT
<b>Next Review Due</b>	30 October 2028
<b>Audience – Training and Awareness Approach</b>	This policy will form part of the Good Governance Guide
<b>Effective Date</b>	30 October 2025
<b>Internal References – Policies &amp; Procedures (Located on HAPI)</b>	Data Protection Policy FOI/SAR & EIR Procedure FOI Policy Fair Processing Notices ICT Security Policy Data Classification Policy Data Breach Procedure
<b>External References</b>	ICO website SFHA Model Documentation

# DATA RETENTION POLICY

---

## 1. Introduction

- 1.1 This policy is designed to ensure that all employees fully understand Hanover's data retention guidelines and consistently apply them in our practices. Data retention is the practice of storing information for a specific period to meet legal, regulatory, and business requirements, such as for audits, legal compliance, or data analytics
- 1.2 This Data Retention Policy applies to all Hanover Employees it sets out what we expect from you in order for Hanover to comply with the GDPR. All Hanover Employees play a vital role in ensuring that Hanover complies with its obligations under the GDPR. You must read and ensure that you fully understand and comply with this policy and all related policies whenever you process personal data on our behalf, and you must attend all related training provided.
- 1.3 Your compliance with this Data Retention Policy and all related policies is mandatory.

## 2. Policy Scope

- 2.1 This policy applies to all Employees, agency workers, volunteers and consultants.
- 2.2 This policy specifies the retention requirements that are to be applied to all of Hanover's information assets, that contain personal data, regardless of what form this asset takes (e.g. paper, electronic records, CD/DVDs, etc.).
- 2.3 **Definitions can be located at Appendix 2** of this policy.

## 3 Responsibility

- 3.1 Compliance to this policy is the responsibility of the Data Protection Officer, supported by the Risk & Governance team. This includes training all employees ensure they are aware of their responsibilities and the internal processes regarding data retention and destruction. Records of this training will be maintained in line with our Data Protection Policy.
- 3.2 The individual information asset owner is responsible for ensuring that the assets they control, should they contain personal data, are only retained for as long as they are required before being destroyed/deleted in a secure manner. The retention periods for different data types are specified at the end of this document.
- 3.3 All data is set out within our departmental Data Asset Registers that states what the data is, who the information asset owner is for the data and the format it is held in. The Data Asset Registers are reviewed at least annually and are available to view on HAPI.
- 3.4 It is the responsibility of all Hanover employees to comply with this policy. Failure to comply with this policy could result in potential enforcement action from regulators, claims from data subjects and reputational damage, in addition to increased costs of storage and the increased workload from handling data subject individual rights requests. Non-compliance with this policy may also lead to disciplinary action.

## 4 Data Principles

- 4.1 All personal data assets must be documented in the Article 30 Record of Processing Activities (ROPA), as required by the UK GDPR. In accordance with Article 5(e), personal data should only be retained for as long as necessary to fulfil the purposes for which it was collected.

## DATA RETENTION POLICY

- 4.2 The retention obligation under the GDPR means in practice that the personal data should not be retained for longer than is necessary for the purposes it has been collected for (as notified to data subjects) unless a valid business reason calls for its continued retention. An example of this might be where there is a legal claim ongoing, anticipated or threatened and personal data which is at the end of its retention period is likely to be relevant to that claim.
- 4.3 For each asset, a business role should be identified that 'owns' the asset. The asset owner is responsible for ensuring that the asset is correctly classified and for the day-to-day maintenance of applicable controls.
- 4.4 Measures must be in place to identify when a retention limit is reached, to ensure that all applicable records can be deleted.
- 4.5 At the end of the retention period for the data, it is the responsibility of the asset owner to ensure that the data is deleted or destroyed in a secure manner so that the data is completely unreadable and cannot be accessed or used for unauthorised purposes. The deletion must also apply to archived or backup copies of the data.
- 4.6 The data asset owner must both sign off and record the deletion of data, including date (time if relevant), content of file and method of deletion or destruction.

In some instances, the destruction of data must be stopped immediately, examples of this are:

- **Legal Holds/Litigation** - If Hanover is involved or anticipates legal proceedings, relevant data must be preserved, even if it has reached its scheduled deletion date.
- **Regulatory or Statutory Requirements** - Laws may mandate keeping data for a longer period (e.g., financial records, tax information, employee data). Example: In many fields, financial transaction data must be kept for 5–7 years.
- **Ongoing Investigations** - Data needed for law enforcement or internal investigations cannot be deleted until the enquiry is complete
- **Audit Requirements** - If data is required for an ongoing or upcoming audit, deletion must be deferred until the audit process is finalised.
- **Contractual Obligations** - Contracts with clients, partners, or vendors may specify retention requirements that override standard deletion schedules.
- **Business-Critical Needs** - In some cases, Hanover may extend retention if data is still needed for operational, historical, or strategic purposes, provided this doesn't conflict with privacy laws.

The destruction of data must stop immediately upon notification from the Risk and Governance Team; destruction may begin again once the Risk & Governance team approves this.

- 4.7 Information asset owners may delegate routine tasks, in respect of the management of their assets or systems in which they are stored or processed.
- 4.8 All new information assets must be added to the ROPA as and when they are acquired and removed from the register when that entire processing activity ceases and data is removed permanently. Asset owners should contact the Risk & Governance team via the Data protection mailbox, noted at 4.6 above to facilitate this.

## DATA RETENTION POLICY

4.9 Should there be any queries around the correct retention limit for a specific asset, these are to be raised with the Risk and Governance team or Data Protection Officer.

### Revision History

Version Number	Revision Date	Approval Date	Approved by	Review Reason
1	October 2019	October 2019		New policy
2	September 2025	30 October 2025	SMT	Revised and updated as part of the GDPR improvement plan

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
	<b>Governance and Management</b>			
GOV1	Certificate of registration as a registered social landlord from SHR	Permanently	Regulatory Requirements	Retain
GOV2	Confirmation of registration as a Scottish charity from OSCR	Permanently	Regulatory Requirements	Retain
GOV3	Confirmation of charitable status from HMRC	Permanently	Regulatory Requirements	Retain
GOV4	Certificate of registration as a registered society with the FCA	Permanently	Regulatory Requirements	Retain
GOV5	Certificate of registration as a care provider with the Care Inspectorate	Permanently	Regulatory Requirements	Retain
GOV6	Certificate of change of Company name	Permanently	Regulatory Requirement - Companies Act	Retain
GOV7	Certification of Registration with Scottish Housing Regulator	Permanently	Housing (Scotland) Acts 2001	Retain
GOV8	Letter of Charitable Recognition/Registration	Permanently	Charities and Trustee Investment (Scotland) Act 2005	Retain
GOV9	Board, AGM and SGM, Committee minutes	Permanently	Regulatory Requirement – Companies Act	Retain
GOV10	Committee minutes	Permanently	Business requirement	Retain
GOV11	Constitutional documents	Permanently	Regulatory Requirement	Retain
GOV12	Applications for membership	5 years after last contact	As per Co-Operative and Community Benefit Societies Act	Confidential destruction
GOV13	Full membership register	Permanently	As per Co-Operative and Community Benefit Societies Act	Retain
GOV14	Register of share certificates	Permanently	As per Co-Operative and Community Benefit Societies Act	Retain

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
GOV15	Board member declarations of interest	5 years after cessation of membership of Board	Usual Practice	Confidential destruction
GOV16	Board member documents, including appointment letters & recruitment files	5 years after cessation of membership of Board	Usual Practice	Confidential destruction
GOV17	Register of payments and benefits	10 years from date of register entry	Usual Practice	Confidential destruction
GOV18	Register of gifts and hospitality	10 years from date of register entry	Usual Practice	Confidential destruction
GOV19	Employee Declaration of Interest Register	10 years from date of register entry	Usual Practice	Confidential destruction
GOV20	Annual return on the Scottish Social Housing Charter, including supporting information	5 years from date of submission	Usual Practice	Confidential destruction
GOV21	5YFP	5 years from date of submission	Usual Practice	Confidential destruction
GOV22	SHR – Loan Portfolio	5 years from date of submission	Usual Practice	Confidential destruction
GOV23	Annual Assurance Statements	5 years from date of submission	Usual Practice	Confidential

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
				destruction
GOV24	Annual return to the FCA	Permanently	Regulatory Requirement	Retain
GOV25	OSCR annual return	Permanently	Regulatory Requirement	Retain
GOV26	Companies House return	Permanently	Regulatory Requirement	Retain
GOV27	Business plans and supporting documentation	5 years from date of completion	Regulatory Requirement	Confidential destruction
GOV28	Current Business continuity plan	Retain indefinitely / until superseded	Best Practice - Ensure accessibility and reference for operational continuity	Confidential destruction
GOV29	Superseded BCP versions	Retain for 6 years after superseded	Aligns with public sector best practice	Confidential destruction
GOV30	Internal Audit Reports	Retain for 6 years	Best practice / in line with financial record-keeping and audit standards	Confidential destruction
GOV31	Strategic Risk Registers	Permanently (as part of Board papers)	Linked to Governance, Board decision-making, or annual planning. They form part of the corporate record and may be required to demonstrate due diligence to regulators, auditors, or in legal proceedings.	Retain

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
GOV32	Details concerning individuals making Subject Access Requests or requests under FOI or the EIRs	5 years from conclusion of request	Prescription & Limitation (Scotland) Act 1973	Confidential destruction
GOV33	Details relating to complaints	Where complainant is a tenant: end of tenancy + 1 year  Where complainant is another type of customer i.e. Telecare Corporate Customer, Telecare Customer, Factored Owner: resolution of complaint + 1 year	Where a complainant is a tenant and has left - retain for 1 year for possibility of return or complaint etc.	Confidential destruction
GOV34	Care Inspectorate Inspection reports	5 years	Regulatory Requirements	Confidential destruction
GOV35	Telephone recordings Hanover only record Hanover Connect calls	2 years	In line with TSA guidance	Automated deletion via software
GOV36	Voicemail recordings	90 days	In line with software capability	Automated deletion via software



## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
GOV 37	Employees Liability Insurance Certificate	40 years	Best practice	Confidential destruction
GOV 38	Insurance Policy Documents	7 years	Best practice	Confidential destruction
GOV39	Insurance <b>Liability Claim</b> documentation	6 years	Best Practice / In line with the Prescription & Limitation (Scotland) Act 1973 Can be extended to 10 years for complex liability cases	Confidential destruction
<b>People &amp; Organisational Development</b>				
HR1	Details concerning employees, former employees and student placements	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973  Personal files including training records and notes of disciplinary and grievance hearings  5 years to cover the time limit for bringing any civil legal action, including contractual claims	Confidential destruction
HR2	New starter information	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR3	Leaver's information	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
HR4	Employee change of details	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR5	Staff training details Includes Asbestos training certificates	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR6	Medical or Stress risk assessment	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR7	Completed Application forms and job pack	If selected - term of employment + 7 years If not selected – 2 years from date of decision	As per Prescription & Limitation (Scotland) Act 1973  Minimum 6 months to a year from date of interviews. Successful applicant's documents should be transferred to personal file.	Confidential destruction
HR8	Interview assessment form	If selected - term of employment + 7 years If not selected – 2 years from date of decision	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR9	Conditional offer request form	Successful candidate: Term of employment + 7 years  Unsuccessful candidate: 2 years from date of decision	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
HR10	Conditional Offer of employment/engagement	Successful candidate: Term of employment + 7 years  Unsuccessful candidate: 2 years from date of decision	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR11	Conditional offer forms (Appendices)	Successful candidate: Term of employment + 7 years  Unsuccessful candidate: 2 years from date of decision	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR12	Employment/Character reference request forms	Successful candidate: Term of employment + 7 years Unsuccessful candidate: 2 years	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR13	Confirmation of appointment/engagement forms (appendices)	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR14	Declaration of physical and mental capacity	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR15	Preferred candidate checklists	2 years	As per Prescription & Limitation (Scotland) Act 1973	Confidential

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
				destruction
HR16	Change of conditions letters	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973	Confidential destruction
HR17	Details concerning agency staff, carers not employed by Hanover and volunteers	3 months	As advised by Head of HR/OD	Confidential destruction
HR18	Statutory Sick Pay records, calculations, certificates, self-certificates	3 years	As advised by Head of HR/OD	Confidential destruction
HR19	Wages/salary records, expenses, bonuses	6 years	As advised by Head of HR/OD	Confidential destruction
HR20	Parental Leave	3 years	Up to 18 years if the child receives a disability allowance, and for a minimum of 5 years in other cases.	Confidential destruction
HR21	Equality Schemes - Includes Gender Pay Gap Statement and Equal Pay Statement and preparatory information	3 years	The Equality Act 2010 (Gender Pay Gap Information) Regulations 2017	Confidential destruction

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
HR22	Identification of documents of foreign nationals (ensuring from the obligation to retain copies of documents used to perform immigration checks)	2 years	Immigrations (Restrictions on Employment Order) 2007/3290 Article 6 (1) (b)	Confidential destruction
HR23	Employment tribunal records	5 years	Prescription and Limitation (Scotland) Act 1973 Nb These records must not be destroyed if a claim has been intimated, there is pending/ongoing employment tribunal, an information request has been intimated, or an audit is ongoing.	Confidential destruction
<b>Finance</b>				
FIN1	Finance reports i.e Management Accounts, Statutory Accounts, External Audit Report	6 years	As per Taxes Management Act 1970	Confidential destruction
FIN2	Overtime Claims	6 years	As per Taxes Management Act 1970	Confidential destruction
FIN3	Expenses Claims	6 years	As per Taxes Management Act 1970	Confidential destruction
FIN4	Pension spreadsheet	Remove employee from spreadsheet when they leave the business	Employee will no longer receive pension contributions from Hanover	Confidential destruction

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
FIN5	Tax submissions	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973 and HMRC requirements	Confidential destruction
FIN6	Deductions from Salaries	Term of employment + 7 years	As per Prescription & Limitation (Scotland) Act 1973 and HMRC requirements	Confidential destruction
FIN7	Supplier invoices	Last interaction with supplier + 1 year	After ceased using supplier retain for 1 year for financial use with completing Tax returns and providing details to ARC	Confidential destruction
FIN8	Details of payments to suppliers	Last interaction with supplier + 1 year	After ceased using supplier retain for 1 year for financial use with completing Tax returns and providing details to ARC	Confidential destruction
FIN9	Details of cheques to be issued for payments	Last interaction with supplier + 1 year	After ceased using supplier retain for 1 year for financial use with completing Tax returns and providing details to ARC	Confidential destruction
FIN10	Credit checking records	Last interaction with supplier + 1 year	After ceased using supplier retain for 1 year for financial use with completing Tax returns and providing details to ARC	Confidential destruction
<b>Procurement</b>				
CPT1	Suppliers' details	Last interaction with supplier + 1 year	Prescription & Limitation (Scotland) Act 1973	Confidential

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
				destruction
CPT2	Registers on procurement Hub	Last interaction with supplier + 1 year	Prescription & Limitation (Scotland) Act 1973	Confidential destruction
CPT3	Tender documents	Company/contractor not selected - 5 years after end of tender exercise Company/contractor selected - 5 years after end of contract	Prescription & Limitation (Scotland) Act 1973	Confidential destruction
CPT4	New contractor packs	Last interaction with contractor + 1 year	After ceased using supplier retain for 1 year for financial use with completing Tax returns and providing details to ARC	Confidential destruction
CPT5	Contracts – servicing and works	Last interaction with contractor + 1 year	After ceased using supplier retain for 1 year for financial use with completing Tax returns and providing details to ARC	Confidential destruction
	<b>ICT</b>			
ICT1	Active directory	Employee drives/mailboxes are disabled on leaving date and the account deleted 2 months following leave date	In line with best practice	Confidential destruction

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
		i.e. someone leaving on 1st Aug will have their account deleted the 1 <sup>st</sup> working day in Oct		
ICT2	Mimecast (emails)	5 years	Proposal of 5 years, but will review once data cleanse complete Data in relation to specific categories will be deleted from Mimecast in line with that retention period	Confidential destruction
ICT3	Personal data held in instant messages (e.g. Teams / meeting recordings)	Automatically deleted after 3 months	Business requirement	Automated deletion
ICT 4	Back-up systems (Barracuda (MS365), server back-up)	1 year from date of back-up	Business Requirement	Automated deletion
	<b>Housing / Tenancy</b>			
HSG1	Successful applicant details	Details held as part of tenant information and disposed following tenancy termination + 1 year	Business requirement	Confidential destruction
HSG2	Unsuccessful or cancelled applicant details	1 year from date of cancellation or determination that application is unsuccessful	Business requirement	Confidential destruction
HSG3	Details of those intending to live with successful applicants	Details held as part of tenant information and disposed following	Business requirement	Confidential destruction



## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
		tenancy termination + 1 year		
HSG4	Details of those intending to live with unsuccessful or cancelled applicants	1 year from date of cancellation or determination that application is unsuccessful	Business requirement	Confidential destruction
HSG5	Tenancy Records	Following the end of tenancy, last interaction with resident + 1 year (except where otherwise provided in this Appendix 1)	Business requirement	Confidential destruction
HSG6	Other customer and resident records	Last interaction with resident [+ 1 year] (except where otherwise provided in this Appendix 1)	Business requirement	Confidential destruction
HSG7	Tenancy debt information	5 years	Business requirement	Confidential destruction
HSG8	New resident details form	Last interaction with resident + 1 year	Business requirement	Confidential destruction
HSG9	Tenancy agreement	One year following cessation of tenancy	Business requirement	Confidential

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
				destruction
HSG10	Stage 3 adaptations applications, grants and documentation	Last interaction with resident + 1 year	Business requirement	Confidential destruction
HSG11	Details concerning Factored Owners and Sharing Owners	Last interaction with owner [+ 1 year] (except where otherwise provided in this Appendix 1)	After provision of services to Factored or Sharing Owners retain for 1 year for possibility of return or complaint etc.	Confidential destruction
HSG12	Anti-Social behavior registers	Remove tenant's details after end of tenancy	<p>After resident has left retain for 1 year for possibility of return or complaint etc.</p> <ul style="list-style-type: none"> <li>• ASB case files</li> <li>• 5 years/end of legal action if any legal action has taken place</li> </ul>	Confidential destruction
HSG13	CCTV Images	<p>30 days.</p> <p>Anything held for more than 3 months will be reviewed.</p>	<p>Business Requirement</p> <p>No more images and information should be stored than that, which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.</p>	Confidential destruction
Care and support				

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
CARE1	Resident independent living assessment form	1 year after tenant has left	After resident has left, retain for 1 year for possibility of return or complaint etc.	Confidential destruction
CARE2	Care plans	1 year after tenant has left	After resident has left retain for 1 year for possibility of return or complaint etc.	Confidential destruction
CARE3	Medication records – MAR sheets, prescriptions	1 year after tenant has left	After resident has left retain for 1 year for possibility of return or complaint etc.	Confidential destruction
CARE4	Risk Assessments	1 year after tenant has left	After resident has left retain for 1 year for possibility of return or complaint etc.	Confidential destruction
CARE5	Personal Evacuation plans	1 year after tenant has left	After resident has left retain for 1 year for possibility of return or complaint etc.	Confidential destruction
CARE6	Housing Support Plans (HSP)	1 year after tenant has left	After resident has left retain for 1 year for possibility of return or complaint etc.	Confidential destruction
	Hanover Connect			

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
TEL1	Residents Telecare details	1 year after tenant has left	After resident has left retain for 1 year for possibility of return or complaint etc.	Confidential destruction
TEL2	Corporate contracts and corporate customer information	1 year after tenant has left	After resident has left retain for 1 year for possibility of return or complaint etc.	Confidential destruction
TEL3	Emergency services information	1 year after tenant has left	After resident has left retain for 1 year for possibility of return or complaint etc.	Confidential destruction
TEL4	Telecare details form/ details	1 year after tenant has left	After resident has left retain for 1 year for possibility of return or complaint etc.	Confidential destruction
TEL5	Keyholder / NOK	1 year after tenant has left	After resident has left retain for 1 year for possibility of return or complaint etc.	Confidential destruction
TEL6	Corporate Customer Contract Management Records i.e <ul style="list-style-type: none"> <li>- Contracts</li> <li>- Performance Meeting Agendas and Outputs</li> <li>- Pricing Details and Decisions</li> <li>- Credit Control Information</li> </ul>	End of contract + 6 years	Prescription & Limitation (Scotland) Act 1973	

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
TEL7	Call recordings	2 years	Deleted after 2 years automatically in line with TSA guidelines	Through TSA guidelines
<b>Health &amp; Safety</b>				
HS1	Accident Incident & near miss information	3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended	Confidential destruction
HS2	General Risk assessments (e.g. coffee mornings, home working, manual handling etc.)	Minimum of 3 years  This is the statute of limitations for a civil claim for a personal injury	Best Practice	Confidential destruction
HS3	Risk Assessment - Lone working	Minimum of 3 years  This is the statute of limitations for a civil claim for a personal injury	Best Practice	Confidential destruction
HS4	Records of equipment given to employees – General Work Equipment (PUWER)	minimum of 3 to 6 years after the employee has left.	Provision and Use of Work Equipment Regulations 1998 (PUWER)	Confidential

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
	Information held in Workrite	This covers the standard time limits for potential legal claims		destruction
HS5	Health and Safety assessments and records of consultations with safety representatives	Permanently	Any HSE or H&S material incident would be reported to Board and as such detailed in the Board minutes which are held permanently as standard	Retain
HS6	Training material for Health & Safety courses	Every 5 years at end of financial year	Health and Safety training material delivered internally (including Fire awareness, manual handling, general Health & Safety, Fire Marshall training) - Business requirement	Confidential destruction
HS7	Reporting: - Accidents and incident reporting - reporting accidents involving adults (including accidents reportable under RIDDOR) - not involving asbestos or a substance hazardous to health	3 years	Prescription and Limitation (Scotland) Act 1973; Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR) SI 2013 No 1471 Regulation 12(2)  These records must not be destroyed if a claim has been intimated, there is pending/ongoing court action, an information request has been intimated or an audit is ongoing	Confidential destruction
HS8	Assessment of the workplace	3 years	Business requirement	Confidential destruction

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
HS9	Monitoring: - Hazardous substances	40 years	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11 Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)  Hazardous substances COSHH Assessments	Confidential destruction
<b>Office Facilities</b>				
FAC1	Visitor logs for offices / locations	3 months automatically deleted for Digital Reception	System capabilities	Confidential destruction
FAC2	Conference centre booking details	Last interaction with client + 1 year	As client may return to use conference centre	Confidential destruction
<b>Communications</b>				
COMM 1	Image library	Where consent relied upon: Until consent is retracted (if image contains personal data)  Where consent is not relied upon: [until image is no longer to be used or subject objects to retention]	If image contains personal data, when consent is retracted then the image must be deleted  If consent is not relied upon image will be retained for as long as purpose for which it was collected is still relevant unless valid	Confidential destruction

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
COMM 2	Customer complaints to the press	3 years	Business requirement	Confidential destruction
COMM 3	Award submissions	5 years	Business requirement	Confidential destruction
COMM 4	Campaigns – final output	5 years	Business requirement	Confidential destruction
<b>Asset Management</b>				
AM1	Property Asbestos surveys <i>Monitoring - Asbestos control</i>	For the lifetime of the property i.e. until property is sold or razed to the ground	Monitoring carried out in accordance with Control of Asbestos Regulations 2012 SI 2012 No 632 Regulation 1	Confidential destruction
AM2	Asbestos Register	Permanently	Business requirement	N/A
AM3	Demolition project records - Health and Safety File	Permanently	These records are live records.  Records such as; -Asbestos air monitoring, survey, geo-tech reports, ground investigations, Plans, Planning Permissions, Building warrants, Completion Certificates, utility disconnection confirmation	Retain
AM4	Demolition project records - contractual correspondence	5 years	These records must not be destroyed if a claim has been intimated, there is pending/ongoing court action, an information request has been intimated or an audit is ongoing.	Confidential destruction



## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
			signed pre-commencement letters, signed stewardship letters, final payment of account from contractor	
AM5	New Build project records - Health and Safety File	Permanently	Business requirement  Records such as;-Asbestos air monitoring, survey, geo-tech reports, ground investigations, Plans, Planning Permissions, Building warrants, Completion Certificates, utility connection confirmation	Retain
AM6	Property security - Records documenting the investigation of a security incident in a property, and action taken.	3 years	Business requirement  Date of completion of investigation	
AM7	Equipment and consumables – stock Stock inventory, stock taking records, condition monitoring, movement of stock	3 years	Business requirement	Confidential destruction
AM8	Electrical Inspection	6 years	Business requirement	Confidential destruction
AM9	Gas CP12 certificates	6 years	Business requirement	Confidential destruction
AM10a	<b>Lift Inspection Documentation –</b> Thorough examination before first use  Lifting Equipment  • Lifting accessories	Until Hanover ceases to use the lifting equipment  2 years	LOLER Regulations	Confidential destruction

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
AM10b	<b>Lift Inspection Documentation</b> – Thorough examination before use where the safety of the equipment depends on the installation conditions	Until the equipment is no longer in use at the place where it was installed/assembled	LOLER Regulations	Confidential destruction
AM10c	<b>Lift Inspection Documentation</b> – In-service thorough examination (6 monthly, 12 monthly, or examination scheme)	Until the next report is made or 2 years – whichever is the later	LOLER Regulations	Confidential destruction
AM10d	<b>Lift Inspection Documentation</b> - In-service inspections/test	Until the next report is made	LOLER Regulations	Confidential destruction
AM11a	<b>Records of equipment given to residents</b> – Standard equipment	6 years after the resident has left or the equipment has been removed	Limitation Act	Confidential destruction
AM11b	<b>Records of equipment given to residents</b> – Smoke Alarms Testing & Inspection records	At least 5 Years	Regulatory Reform (Fire Safety) Order 2005 (RRO) / BS 5839-6:2019 / BS 5839-6 Category LD1 or LD2 systems	Confidential destruction
AM11c	<b>Records of equipment given to residents</b> – Smoke Alarms Install & commissioning records	Lifetime if the system + 5 years	As above	Confidential destruction
AM11d	<b>Records of equipment given to residents</b> – Smoke Alarms Servicing & maintenance logs	At least 5 Years	As above	Confidential destruction
AM12	Water Hygiene Assessment Certificates	At least 5 Years  For as long as they are current + at least 2	Best Practice	Confidential destruction

## DATA RETENTION POLICY

	Type of Data & Team	Recommended Retention period	Rationale	Disposal Action
	Water Hygiene Policy & procedure documents	further years after superseded		

Appendix 2

## GDPR Definitions

<b>Data Subjects</b>	A <b>data subject</b> is any individual whose personal data is being collected, stored, or processed by an organisation.
----------------------	--

## DATA RETENTION POLICY

	<p>Personal data refers to any information that can be used to identify a person, such as:</p> <ul style="list-style-type: none"><li>• Name</li><li>• Email address</li><li>• Phone number</li><li>• Location data</li><li>• IP address</li><li>• Biometric data</li></ul>
<b>Asset Owner</b>	<p>An asset owner is the person, group, or organisation that has legal ownership and ultimate accountability for an asset.</p> <ul style="list-style-type: none"><li>• The <b>asset owner</b> is responsible for the value, use, and protection of the asset.</li><li>• They make decisions about how the asset is acquired, maintained, used, or disposed of.</li></ul>
<b>Information Asset</b>	<p>An <b>information asset</b> refers to any data, information, or knowledge that has value to an organisation and is used to achieve its objectives. Information assets can be in various forms - physical or digital - and include both raw data as well as processed and analysed information. These assets are vital for decision-making, operations, and maintaining competitive advantage.</p>
<b>ROPA</b>	<p>A <b>ROPA</b> stands for <b>Record of Processing Activities</b>. It is a document or record required by the <b>General Data Protection Regulation (GDPR)</b> for organisations that process personal data. The purpose of the ROPA is to provide transparency and accountability regarding how personal data is processed within an organisation.</p>